UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA

APRIL BUTLER, *individually and on behalf of all others similarly situated*, Plaintiff, v. ACADIAN AMBULANCE SERVICE, INC., Defendant.	DOCKET: SECTION: MAGISTRATE: **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff April Butler ("Plaintiff"), on behalf of herself and all others similarly situated ("Class Members"), alleges the following against Defendant Acadian Ambulance Service, Inc. ("Defendant"), upon Plaintiff's personal knowledge and upon information and belief, including the investigation of counsel.

I. INTRODUCTION

1. This action arises from Defendant's failure to safeguard the sensitive personally identifiable information[1] ("PII") and protected health information ("PHI") (PII and PHI together, "Private Information") of Plaintiff and the proposed Class Members, millions of Defendant's current and former patients. Specifically, between February 29, 2024, and March 2, 2024, the notorious criminal ransomware group known as Daixin accessed Defendant's network systems and exfiltrated Plaintiff's and Class Members' Private Information stored therein, including their

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

names, dates of birth, Social Security numbers, medical records, case histories, physicians' notes, suspected drug use, employment information, and other confidential personal information, causing widespread injuries and damages to Plaintiff and Class Members (the "Data Breach").

2. According to its website, Defendant provides air and ground emergency medical transportation and services to millions of patients across Louisiana, Mississippi, Tennessee, and Texas.[2]

3. As a condition of receiving medical services from Defendant, Plaintiff and Class Members were required to entrust Defendant with their sensitive Private Information including their names, dates of birth, Social Security numbers, medical records, case histories, physicians' notes, suspected drug use, laboratory test results, and other confidential personal information.

4. As the custodian of Plaintiff's and Class Members' Private Information it collected and maintained, Defendant had a duty to adopt reasonable measures to protect such Private Information from involuntary disclosure to unauthorized third parties, and to keep it safe and confidential. Defendant had obligations under contract, statutory and common law, industry standards, and representations made to Plaintiff and Class Members to keep their Private Information secure and to protect it from unauthorized access and disclosure.

5. Defendant breached these duties owed to Plaintiff and Class Members by failing to safeguard their Private Information it collected and maintained, including by failing to implement industry standards for data security to protect against cyberattacks, resulting in the Data Breach. Defendant could have prevented the Data Breach by implementing standard and reasonable data security measures but failed to do so.

6. As a direct result of the Data Breach, which Defendant failed to take reasonable

[2] *See* https://acadianambulance.com/our-company/our-history/ (last visited August 2, 2024).

steps to prevent, the Private Information of Defendant's patients, including Plaintiff and Class Members, was stolen into the hands of notorious cybercriminals.

7. According to Defendant's pre-prepared media statement dated July 25, 2024, the Data Breach occurred "earlier this year" when unidentified cybercriminals accessed Defendant's server and stole files containing Plaintiff's and Class Members' Private Information stored therein.[3]

8. Plaintiff since discovered that the Daixin ransomware group accessed and exfiltrated over 10 million patients' Private Information in the Data Breach and has now published the stolen Private Information on its Dark Web page.

9. Daixin's Dark Web post indicates it accessed Plaintiff's and Class Members' Private Information from Defendant's server in or before June 2024. According to information Daixin provided to the blog DataBreaches.net, Daixin began communicating with Defendant about the Data Breach on or about June 22, 2024, threatening to publish all Private Information stolen in the Data Breach on its Dark Web page unless Defendant paid a $7 million ransom.[4]

10. Thus, Defendant has known since at least June 22, 2024, that a cybercriminal organization accessed millions of its patients' Private Information in the Data Breach. Yet, to date Defendant has failed to provide Plaintiff, Class Members, or the public *any* meaningful information about the Data Breach, like the extent of Private Information involved, the amount of individuals affected, or the fact that Daixin has now published millions of Defendant's patients' sensitive Private Information on the Dark Web.

---

[3] Michael Sipes, Acadian Ambulance says cyber attack gained access to protected health information, KLFY (July 26, 2024), https://www.klfy.com/local/acadiana-ambulance-says-a-cyber-attack-gained-access-to-protected-health-information/.

[4] Dissent, *Acadian Ambulance hit by ransomware attack; Daixin claims info on 10 million patients stolen*, DataBreaches.net (July 23, 2024), https://databreaches.net/2024/07/23/acadian-ambulance-hit-by-ransomware-attack-daixin-claims-info-on-10-million-patients-stolen/.

11. Plaintiff and Class Members now face a lifetime risk of identity theft due to the nature of the Private Information stolen and now disseminated, which they cannot change, and which cannot be made private again.

12. Defendant's harmful conduct has injured Plaintiff and Class Members in multiple ways, including, *inter alia* (i) actual identity theft, and the imminent risk thereof; (ii) the lost or diminished value of their Private Information; (iii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) out-of-pocket expenses and lost opportunity costs to mitigate the Data Breach's consequences, including lost time; (v) loss of privacy, including through the publication and dissemination of their Private Information on the Dark Web; (vi) loss of the benefit of their bargain with Defendant; and (vi) emotional distress associated with the loss of control over their highly sensitive Private Information and attendant, certain risk of identity theft and fraud.

13. Defendant's failure to protect Plaintiff's and Class Members' Private Information has harmed and will continue to harm thousands of Defendant's current and former patients, causing Plaintiff to seek relief on a class-wide basis.

14. Plaintiff brings this action individually and on behalf of all others similarly situated, the proposed Class of individuals whose Private Information was compromised in the Data Breach, asserting causes of action for (I) Negligence/Negligence *Per Se*; (II) Breach of Implied Contract; (III) Breach of Fiduciary Duty; (IV) Unjust Enrichment; (V) Invasion of Privacy/Intrusion Upon Seclusion; and (VI) Declaratory/Injunctive Relief, seeking damages and equitable relief due to Defendant's failure to protect Plaintiff's and Class Members' highly sensitive Private Information.

II. PARTIES

15. Plaintiff April Butler is a natural person, resident, and citizen of Texas. Plaintiff is a former patient of Defendant and a victim of Defendant's Data Breach.

16. Defendant Acadian Ambulance Service, Inc. is a corporation company formed under Louisiana law and headquartered at 130 East Kaliste Saloom Road, Lafayette, LA 70508.

III. JURISDICTION AND VENUE

17. This Court has personal jurisdiction over Defendant because it is a Louisiana corporation with its principal place of business is in Louisiana and, personally or through its agents, it engages in substantial and continuous activities in Louisiana and conducts business in this state.

18. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because the amount in controversy exceeds $5 million, exclusive of interest and costs, the number of Class Members is over 100, and at least one Class Member (namely, Plaintiff) is a citizen of a state that is diverse from Defendant's citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. The Court has supplemental jurisdiction over Plaintiff's claims arising under state law pursuant to 28 U.S.C. § 1367.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant has its principal place of business located in this District, and a substantial part of the events giving rise to this action and Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Defendant's Business

21. According to its website, Defendant is "one of the nation's most respected and largest privately held medical transportation companies," with operations in "more than 70 parishes and counties that are home to more than 24 million residents in Louisiana, Mississippi, Tennessee

and Texas."[5]

22. As a condition of receiving healthcare services from Defendant, Plaintiff and Class Members were required to entrust Defendant with their sensitive Private Information including their names, dates of birth, Social Security numbers, medical records, case histories, physicians' notes, drug use information, laboratory test results, and other confidential personal information, and did in fact turn over such Private Information to Defendant.

23. In exchange for receiving Plaintiff's and Class Members' Private Information, Defendant promised to safeguard the sensitive, confidential data and to only use it for authorized and legitimate purposes.

24. The data held by Defendant and accessed in the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

25. Defendant made promises to Plaintiff and Class Members to adequately maintain and protect their Private Information, demonstrating its understanding of the importance of such data's integrity.

26. Defendant made promises and representations to its patients, including Plaintiff and Class Members, that the Private Information it collected from them would be kept safe and confidential, that the information's privacy would be maintained, and that Defendant would delete any sensitive information once no longer required to keep it it.

27. Indeed, Defendant's Notice of Privacy Practices, published on its website and, upon information and belief, provided to all patients receiving services from Defendant, warrants that the Private Information Defendant collects from its patients will be used or disclosed only for specific enumerated reasons, "usually in ways that contribute to the public good," and none of

[5] *See* https://acadianambulance.com/our-company/our-history/ (last visited August 2, 2024).

which include exposure to criminal ransomware organizations or publication on the Dark Web.[6]

28. Defendant's Notice of Privacy Practices further promises as follows:

> Our Responsibilities
>
> - We are required by law to maintain the privacy and security of your protected health information.
> - We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
> - We must follow the duties and privacy practices described in this notice and give you a copy of it.
> - We will not use or share your information other than as described here unless you tell us we can in writing.[7]

29. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its promises to safeguard that information, including in the manners set forth in Defendant's Notice of Privacy Practices.

30. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to Plaintiff and Class Members, and knew or should have known that it was responsible for protecting their Private Information from unauthorized disclosure.

32. Moreover, Defendant had and has duties to adopt reasonable measures to keep Plaintiff's and Class Members' Private Information confidential and protected from involuntary disclosure to third parties, and to audit, monitor, and verify the integrity of its data management

---

[6] *Acadian Ambulance Service, Inc. Notice of Privacy Practices*, available at https://acadian.com/wp-content/uploads/Noticy-of-Privacy-Practices.pdf (last visited August 2, 2024).

[7] *Id.*

systems and those its affiliates. Such duties arise from common law, the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45 ("FTC Act"), HIPAA, 45 C.F.R. § 160.102, contract, industry standards, and representations made to Plaintiff and Class Members to keep their Private Information confidential and protected from unauthorized access and disclosure.

33. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard it.

34. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

35. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use it for necessary purposes only, and to make only authorized disclosures of this information. Defendant failed to do so.

Defendant Failed to Adequately Safeguard Plaintiff's and Class Members' Private Information, causing the Data Breach.

36. Defendant collected and maintained its current and former patients' Private Information in its information technology networks and servers, including when the Data Breach occurred.

37. The information held by Defendant at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

38. On or before June 22, 2024, the notorious ransomware group Daixin accessed Defendant's network servers and exfiltrated Plaintiff's and Class Members' unencrypted Private Information stored therein.

39. The files Daixin obtained from Defendant contained multiple tables with over 11

million lines of patient data including patient names, dates of birth, contact information, Social Security numbers, medical and case histories, physician notes and documentation, suspected drug use, infectious disease status, employment information, medical symptoms, and other sensitive and confidential PII and PHI.

40. Defendant has failed to provide Plaintiff and Class Members any meaningful information or details about the Data Breach whatsoever, beyond the fact that it occurred and that its patients' Private Information was compromised therein. Defendant's completely deficient notice omits critical facts like the extent of Private Information compromised in the Data Breach, or that it was accessed by the Daixin cybercriminal group and is now published it on the Dark Web.

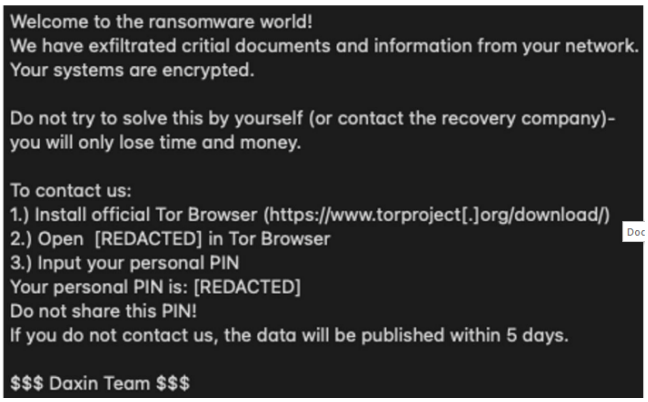
41. According to an October 2022 Joint Cybersecurity Advisory ("CSA") whitepaper,

> The Daixin Team is a ransomware and data extortion group that has targeted the HPH [(Healthcare and Public Health)] Sector with ransomware and data extortion operations since at least June 2022. Since then, Daixin Team cybercrime actors have caused ransomware incidents at multiple HPH Sector organizations where they have . . . [e]xfiltrated personal identifiable information (PII) and patient health information (PHI) and threatened to release the information if a ransom is not paid.[8]

42. The CSA whitepaper includes the following example of a Daixin ransom note following a cyberattack like this Data Breach[9]:

[8] *#StopRansomware: Diaxin Team*, CSA (October 21, 2022), available at https://www.aha.org/system/files/media/file/2022/10/joint-cybersecurity-advisory-tlp-white-stop-ransomware-daixin-team-10-21-22.pdf.

[9] *Id.*



43. Defendant did not use reasonable security procedures and practices appropriate to the sensitive and confidential nature of Plaintiff's and Class Members' Private Information it collected and maintained, such as encrypting the information or deleting it when it is no longer needed, which caused that Private Information's wrongful disclosure in the Data Breach.

44. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing Plaintiff's and Class Members' Private Information and training its employees on standard cybersecurity practices.

45. For example, if Defendant had of implemented industry standard logging, monitoring, and alerting systems—basic technical safeguards that any healthcare provider or PII/PHI-collecting company like Defendant is expected to employ—then cybercriminals would not have been able to perpetrate their malicious activity in Defendant's servers without alarm bells going off, including the reconnaissance necessary to identify where Defendant stored Private Information, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data, staging data in preparation for exfiltration, and then exfiltrating that data outside of Defendant's system without being caught.

46. The activities detailed in the preceding paragraph would have been recognized by Defendant if it bothered to implement basic monitoring and detection systems, which then would have stopped the attack or greatly reduced its impact.

47. Additionally, according to CSA's *#StopRansomware: Daixin Team* whitepaper, "Daixin actors gain initial access to victims through virtual private network (VPN) servers," commonly "acquir[ing] the VPN credentials through the use of a phishing email with a malicious attachment."[10]

48. Phishing is a tactic that uses social engineering to send emails containing malicious attachments to targeted organizations or individuals,[11] and relies on user execution (like opening an email or downloading an attachment) to gain access.[12]

49. Had Defendant trained its employees on reasonable and basic cybersecurity topics, like common phishing techniques or indicators of a potentially malicious event, Daixin would not have been able to carry out the Data Breach through phishing.

50. As a result of Defendant's failures, Plaintiff's and Class Members' Private Information was stolen in the Data Breach when criminal hackers accessed and acquired files in Defendant's network servers storing that sensitive information in unencrypted form.

51. Defendant's tortious conduct and breach of contractual obligations, as detailed herein, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed Plaintiff's and Class Members' Private Information, meaning Defendant had no effective means in place to detect and prevent attempted cyberattacks.

52. To make matters worse, Defendant has yet to provide any meaningful warning, notice, or information whatsoever to Plaintiffs, Class Members, or the public regarding relevant details about the Data Breach like the extent of Private Information compromised or that it was

---

[10] *Id.*

[11] *See* Phishing, MITRE ATT&CK (March 1, 2024), available at https://attack.mitre.org/versions/v15/techniques/T1566/ (last accessed July 9, 2024).

[12] *See* Phishing, MITRE ATT&CK (April 12, 2024), available at https://attack.mitre.org/versions/v15/techniques/T1204/ (last accessed July 9, 2024).

accessed by a notorious cybercriminal organization that has now published it on the Dark Web.

53. Defendant's deficient and indeed, non-existent notice exacerbated Plaintiff's and Class Members' injuries and caused additional damages by depriving them of the opportunity to timely mitigate harm from the Data Breach.

54. Moreover, in the aftermath of the Data Breach, Defendant has not indicated any measures it has taken to mitigate the harm or prevent future breaches of its systems or whether it has remedied the deficiencies that resulted in the Data Breach. Nor has Defendant offered affected individuals any redress or compensation for harm the Data Breach has caused or will cause them.

Defendant Knew or Should Have Known of the Risk of a Cyber Attack Because Healthcare Providers like Defendant in Possession of Private Information are Particularly Suspectable.

55. Defendant's negligence, including its gross negligence, in failing to safeguard Plaintiff's and Class Members' Private Information is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

56. Private Information of the kind accessed in the Data Breach is of great value to hackers and cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the Dark web.

57. Indeed, Daixin's Dark Web page, where the files stolen in the Data Breach are posted, touts that with the Private Information bad actors "can commit a variety of crimes including, e.g. opening new financial accounts, taking out loans, using health information to target other phishing and hacking intrusions based on their individual health needs, using information to obtain government benefits, filing fraudulent tax returns using the information, obtaining driver's licenses in names but with another person's photograph, and giving false information to police during an arrest."

58. Private Information can also be used to distinguish, identify, or trace an individual's identity, such as his or her name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal or identifying information connected or linked to an individual such as his or her birthdate, birthplace, and mother's maiden name.

59. Data thieves regularly target entities in the healthcare industry like Defendant due to the highly sensitive information they maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize it through unauthorized access.

60. Cyber-attacks against institutions such as Defendant are targeted and frequent. According to Contrast Security's 2023 report, "Cyber Bank Heists: Threats to the financial sector," "[o]ver the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[13]

61. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or, if acting as a reasonable healthcare provider, should have known that the Private Information it collected and maintained would be targeted by cybercriminals.

62. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020.

[13] Tom Kellermann, *Cyber Bank Heists: Threats to the financial sector*, at 5, CONTRAST SECURITY https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%2020 23.pdf (last accessed July 8, 2024).

The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[14]

63. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[15]

64. Defendant's data security obligations were particularly important given the substantial increase, preceding the date of the subject Data Breach, in cyberattacks and/or data breaches targeting healthcare entities like Defendant that collect and store PHI.

65. For example, of the 1,862 data breaches recorded in 2021, 330 of them, or 17.7%, were in the healthcare industry.[16]

66. The 330 breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[17]

67. Entities in custody of PHI, like Defendant, reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[18] Indeed, when compromised, healthcare related data is among the most sensitive and personally

---

[14] *See* Identity Theft Resource Center, *2021 Annual Data Breach Report Sets New Record for Number of Compromises*, ITRC (Jan.24, 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

[15] IBM, *Cost of a data breach 2022: A million-dollar race to detect and respond*, https://www.ibm.com/reports/data-breach (last accessed July 8, 2024).

[16] Identity Theft Resource Center, *2021 Data Breach Annual Report*, ITRC (Jan. 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

[17] *Id.*

[18] *See* Identity Theft Resource Center, *2022 Annual Data Breach Report*, ITRC (Jan. 2023) https://www.idtheftcenter.org/publication/2022-data-breach-report.

consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[19] Almost fifty percent of the victims lost their healthcare coverage as a result of the incident, while nearly thirty percent said their insurance premiums went up after the event. Forty percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy.[20]

68. Thus, the healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[21]

69. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[22] A complete identity theft kit with health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[23]

70. Indeed, cyberattacks by the Daixin group in particular, such as this Data Breach,

---

[19] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.
[20] *Id.*
[21] *9 reasons why healthcare is the biggest target for cyberattacks*, SECURESWIVEL, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks (last accessed July 8, 2024).
[22] IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows* (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.
[23] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world* (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

are a specifically known and acknowledged risk for businesses in the healthcare industry like Defendant. According to the CSA whitepaper, cybercriminals like Daixin "routinely target HPH [Healthcare and Public Health] Sector organizations," and Daixin in particular has "caused ransomware incidents at multiple HPH Sector organizations" since June 2022.[24]

71. As a healthcare entity in possession of its patient customers' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members because of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach or the foreseeable injuries it caused.

72. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' Private Information from being compromised.

73. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals, including Daixin specifically, for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names—malicious uses that Daixin specifically references in marketing Plaintiff's and Class Members' Private Information on the Dark Web.

74. Defendant was, or should have been, fully aware of the unique type and the

[24] *#StopRansomware: Diaxin Team*, CSA (October 21, 2022), available at https://www.aha.org/system/files/media/file/2022/10/joint-cybersecurity-advisory-tlp-white-stop-ransomware-daixin-team-10-21-22.pdf.

significant volume of data on Defendant's server(s), amounting to thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

75. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that information.

76. The breadth of data compromised in the Data Breach makes the information particularly valuable to bad actors and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

Defendant is Required but Failed to Comply with FTC Rules and Guidance.

77. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

78. In 2016, the FTC updated its publication *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses like Defendant. Per these guidelines, businesses should protect the personal information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[25]

79. The FTC guidelines also recommend that businesses use an intrusion detection

[25] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.[26]

80. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

81. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures business like Defendant must undertake to meet their data security obligations.

82. Such FTC enforcement actions include actions against healthcare entities like Defendant. *See, e.g.*, *In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

83. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC

[26] *Id.*

publications and orders described above are also part of the basis of Defendant's duty in this regard.

84. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[27]

85. Defendant failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

86. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

Defendant is Required but Failed to Comply with HIPAA Guidelines.

87. Defendant is a covered entity under HIPAA, 45 C.F.R. § 160.102, and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E; and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C.

88. Defendant is further subject to the Health Information Technology Act ("HITECH")'s rules for safeguarding electronic forms of medical information. *See* 42 U.S.C. §17921; 45 C.F.R. § 160.103.

89. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting PHI that is kept or transferred in electronic form.

[27] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

90. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

91. HIPAA's Security Rule required and requires that Defendant do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

92. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. §164.312(a)(1).

93. HIPAA and HITECH also obligate Defendant to implement procedures to prevent, detect, contain, and correct data security violations and disclosures of PHI that are reasonably anticipated but not permitted by privacy rules. *See* 45 C.F.R. § 164.306(a)(1), (a)(3).

94. HIPAA further requires a covered entity like Defendant to have and apply

appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. See 45 C.F.R. § 164.530(e).

95. HIPAA further requires a covered entity like Defendant to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

96. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." U.S. Department of Health & Human Services, Security Rule Guidance Material.[28] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology, which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." U.S. Department of Health & Human Services, Guidance on Risk Analysis.[29]

97. As alleged herein, Defendant failed to comply with HIPAA and HITECH. It failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach, and failed to ensure the confidentiality and protection of

[28] https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed July 8, 2024).
[29] *Id.*

Plaintiff's and Class Members' Private Information, including their most personal PHI.

Defendant Failed to Comply with Industry Standards.

98. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

99. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[30]

100. The NIST also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

[30] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Feb. 9, 2024).

> g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[31]

101. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[32]

102. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7,

---

[31] Federal Trade Commission, *Understanding the NIST Cybersecurity Framework*, FTC.GOV, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last accessed July 8, 2024).

[32] Cybersecurity & Infrastructure Security Agency, *Shields Up: Guidance for Organizations*, https://www.cisa.gov/shields-guidance-organizations (last accessed July 8, 2024).

DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as other industry standards for protecting Private Information, resulting in the Data Breach.

Defendant Owed a Common Law Duty to Safeguard Private Information.

103. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant's duty owed to Plaintiff and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected Plaintiff's and Class Members' Private Information.

104. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

105. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

106. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

107. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

108. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

109. Defendant tortiously failed to take the precautions required to safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized disclosure. Defendant's actions and omissions represent a flagrant disregard of Plaintiff's and Class Members' rights.

Plaintiff and Class Members Suffered Damages.

110. Defendant's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' Private Information directly and proximately injured Plaintiff and Class Members by the consequential disclosure of their Private Information to a criminal ransomware group in the Data Breach.

111. Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to (a) closely monitor their medical statements, bills, records, and credit and financial accounts; (b) change login and password information on any sensitive account even more frequently than they already do; (c) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (d) search for suitable identity theft protection and credit monitoring services and pay to procure them.

112. The unencrypted Private Information of Plaintiff and Class Members compromised in the Data Breach has ***already*** been published on the Dark Web by Daixin. This Private Information published on the Dark Web includes files with millions of lines of Plaintiff's and Class Members' sensitive Private Information. Bad actors with nefarious intentions can now easily access Plaintiff's and Class Members' Private Information—and have done so already.

113. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen,

fraudulent use of that information and damage to victims may continue for years.

114. Once Private Information is exposed, virtually no way exists to ensure that the exposed information has been fully recovered or contained against future misuse. Thus, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, due to Defendant's conduct that caused the Data Breach. Further, the value of Plaintiff's and Class Members' Private Information has been diminished by its wrongful exposure.

115. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of Private Information.

116. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud–a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[33]

117. With respect to healthcare breaches, one study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[34]

118. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[35]

119. The reality is that cybercriminals seek nefarious outcomes from a data breach" and

[33] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last accessed July 8, 2024).
[34] Heather Landi, *More than 70% of hospital data breaches compromise information that puts patients at risk of identity theft* (Sept. 23, 2019, 5:00 PM), https://www.fiercehealthcare.com/tech/more-than-70-hospital-data-breaches-expose-sensitive-information-putting-patients-at-risk.
[35] *Id.*

"stolen health data can be used to carry out a variety of crimes."[36]

120. Health information in particular is likely to be used in detrimental ways, including by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[37]

121. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[38]

122. Plaintiff and Class Members are also at a continued risk because their Private remains in Defendant's servers, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate data security and training measures to protect its patients' Private Information.

Plaintiff's Experience

123. Plaintiff is a former patient of Defendant and received medical services from Defendant prior to the Data Breach.

124. As a material condition of receiving healthcare services from Defendant, Plaintiff was required to provide Defendant with her Private Information, including her full name, date of birth, contact information, Social Security number, physicians' documentation, medical and case history, and other personal and confidential information.

125. At the time of the Data Breach, Defendant retained Plaintiff's Private Information in its network server(s). Upon information and belief, Plaintiff's Private Information was accessed

[36] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[37] *Id.*
[38] https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

and compromised in the Data Breach and has now been published on the Dark Web.

126. Plaintiff has spent considerable time and effort attempting to the Data Breach's harmful effects and prevent fraudulent misuse of her Private Information and attendant damages, as well as time and effort to monitor her accounts to protect herself from additional identity theft.

127. Additionally, Plaintiff's Private Information that was compromised in the Data Breach has already been misused to commit identity fraud. Plaintiff recently learned that an unknown actor misused Plaintiff's Private Information without her authorization to purchase health insurance in Plaintiff's name in Florida, causing Plaintiff to lose her own health insurance coverage in Texas, where she resides.

128. Plaintiff fears that her personal financial security is at substantial risk and because of the uncertainty over the information compromised in the Data Breach. She is experiencing feelings of anxiety, stress, and fear because of the Data Breach, which has manifested into sleep disruption. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim the law provides redress for.

129. Plaintiff was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive Private Information and posting it on the Dark Web, available to any criminal to use to commit further identity theft against Plaintiff. This has been compounded by Defendant's delay in notifying Plaintiff of the Data Breach. Plaintiff has had to expend the above time and effort to rectify the impacts of the Data Breach and does not know how many more identity theft attempts may arise for her lifetime.

130. Due to Defendant's inadequate data security practices and the resulting Data Breach, Plaintiff faces a lifetime risk of further identity theft, as the Private Information stolen includes sensitive data that cannot be changed, like her Social Security number and medical history.

V. COMMON INJURIES AND DAMAGES

131. As the direct and proximate result of Defendant's ineffective and inadequate data security practices and the resulting Data Breach, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

132. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including but not limited to (a) invasion of privacy; (b) out of pocket costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) out of pocket costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) loss of the benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in Defendant's possession and subject to further breaches, so long as Defendant fails to undertake adequate measures to protect it.

The Risk of Identity Theft to Plaintiff and Class Members is Present and Ongoing.

133. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the data by selling it on the black market to other criminals, who then use it to commit a variety of identity theft related crimes discussed below.

134. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take

on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

135. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

136. Daixin's Dark Web page specifically refers to social engineering as a potential use of the Private Information stolen in the Data Breach, suggesting that criminals can "us[e] health information to target other phishing and hacking instructions based on [the victim's] individual health needs."

137. The Dark Web is an unindexed layer of the internet that requires special software or authentication to access.[39] Criminals in particular favor the Dark Web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, Dark Web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[40] This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

138. A sophisticated black market exists on the dark web where criminals can buy or sell

[39] Louis DeNicola, *What Is the Dark Web?*, EXPERIAN (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web.
[40] *Id.*

malware, firearms, drugs, and frequently, personal and medical information like the Private Information at issue here. The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information. In other words, "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[41]

139. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[42]

140. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of

[41] *What is the Dark Web?*, MICROSOFT 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[42] Social Security Administration, *Identity Theft and Your Social Security Number*, SSA.GOV (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

141. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[43]

142. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture, use the victim's name and Social Security number to obtain government benefits, or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for credit lines.[44]

143. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[45]

144. One such example of criminals using Private Information for profit is the development of "Fullz" packages. Cyber-criminals can cross-reference two sources of Private

[43] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.
[44] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[45] *See* Federal Trade Commission, Medical Identity Theft (May 2021), http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

145. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as identity thieves or illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and Class Members' stolen Private Information is being misused, and that such misuse is traceable to the Data Breach.

146. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[46]

147. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[47] Defendant did not rapidly report to Plaintiff and the Class that their Private Information was wrongfully disclosed.

148. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts

[46] *See 2019 Internet Crime Report Released* (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.
[47] *Id.*

or misuse of existing accounts.

149. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

150. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiff and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

151. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm–yet the asset of time has been lost.

152. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

153. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[48] Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[49]

Diminution of Value of the Private Information

154. Private Information is a valuable property right.[50] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

155. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed

[48] *See* U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, at 2 (June 2007), https://www.gao.gov/new.items/d07737.pdf ("GAO Report").
[49] *See* Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed July 8, 2024).
[50] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PRIVATE INFORMATION") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PRIVATE INFORMATION, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

PHI to adjust their insureds' medical insurance premiums.

156. Private Information can sell for as much as $363 per record according to the Infosec Institute.[51]

157. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data sells on the dark web for $50 and up.[52]

158. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[53] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[54] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[55]

159. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized release onto the Dark Web, where it is now available for additional criminals to access and holds significant value for the threat actors.

Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

160. To date, Defendant has done nothing to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach.

---

[51] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market.
[52] *Ransomware attacks paralyze, and sometimes crush, hospitals*, SOPHOS NEWS (Oct. 3, 2019), https://news.sophos.com/en-us/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals
[53] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak* (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[54] https://datacoup.com/.
[55] Nielsen Computer & Mobile Panel, Frequently Asked Questions, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

161. Daixin has already published Private Information exfiltrated in the Data Breach on the Dark Web. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been or will be further disseminated on the black market/Dark Web for sale and purchase by bad actors intending to utilize the Private Information for identity theft crimes (*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money, filing false tax returns, taking out loans or lines of credit, or filing false unemployment claims).

162. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

163. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[56] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers and medical histories).

164. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

165. The retail cost of credit monitoring and identity theft monitoring can cost $200 or

[56] *See* Jesse Damiani, *Your Social Security Number Costs $4 On the Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss of Benefit of the Bargain

166. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain.

167. When agreeing to provide their Private Information, which was a condition precedent to obtain healthcare services from Defendant, and paying Defendant, directly or indirectly, for its services, Plaintiff and Class Members, as Defendant's patients, understood and expected that they were, in part, paying for services and data security to protect the Private Information they were required to provide.

168. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

Lack of Compensation

169. Defendant has offered nothing to compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and entirely fails to provide any redress for the unauthorized disclosure of Plaintiff's and Class Members' Private Information or the costs and time they now must spend attempting to mitigate their injuries.

170. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

171. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, imminent, and substantial risk of fraud and identity theft.

172. Further, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach and face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

173. Specifically, victims suffered and will suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying fees for late or declined payments fees imposed for failed automatic payments tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

174. In addition, Plaintiff and Class Members suffered a loss of value of their Private Information when it was acquired by cyberthieves in the Data Breach. Numerous courts have recognized the property of loss of value damages in related cases.

175. Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

Injunctive Relief is Necessary to Protect Against Future Data Breaches.

176. Moreover, Plaintiff and Class Members have an interest in ensuring that Private Information, which is believed to remain in Defendant's possession, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to employee training on cybersecurity awareness and prevention measures, storing data or documents containing Private Information so they are not accessible online, and ensuring that access to such data is password-protected.

177. Because of Defendant's failure to use reasonable measures to prevent the Data Breach, Plaintiff and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses and lost time. Also, they suffered or are at a materially increased risk of imminently suffering

a. loss of control over how their Private Information is used;

b. diminution in value of their Private Information;

c. compromise and continuing publication of their Private

Information;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. unauthorized use of their stolen Private Information; and

g. continued risk to their Private Information, which remains in Defendant's possession and is thus at risk for futures breaches so long as Defendant fails to take appropriate measures to protect it.

VI. CLASS ALLEGATIONS

178. Plaintiff brings this nationwide class action individually and on behalf of all other persons similarly situated ("Class") pursuant to Federal Rule of Civil Procedure 23(a) and 23(b)(3).

179. Plaintiff proposes the following nationwide Class definition, subject to amendment based on information obtained through discovery:

> All individuals whose Private Information may have been accessed and/or acquired in Defendant's Data Breach beginning on or before June 21, 2024.

180. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

181. Plaintiff reserves the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

182. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Class Members' claims on a class-wide basis using the same

evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

183. This action satisfies the requirements for a class action under Federal Rule of Civil Procedure 23(a)(1)–(3) and 23(b)(2), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

184. **Numerosity, Rule 23(a)(1):** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Private Information of approximately 10 million patients of Defendant was compromised in the Data Breach. Such information is readily ascertainable from Defendant's records.

185. **Commonality, Rule 23(a)(2):** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act and HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether hackers obtained Plaintiff's and Class Members' Private Information in the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

h. Whether Defendant breached the covenant of good faith and fair dealing implied in its contracts with Plaintiff and Class Members; and

i. Whether Plaintiff and the Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

186. **Typicality, Rule 23(a)(3):** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

187. **Adequacy, Rule 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel is competent and experienced in litigating data breach class actions.

188. **Predominance, Rule 23(b)(3):** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and all Class Members' Private Information was stored on the same computer systems and unlawfully exposed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single

action has important and desirable advantages of judicial economy.

189. **Superiority, Rule 23(b)(3):** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions.

b. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

c. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

d. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class

Members and as to Defendant.

190. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only Defendant's patients, the legal and factual issues are narrow and easily defined, and the Class Membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

191. In addition, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

192. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely and adequately notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard

patients' Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

193. Finally, all members of the proposed Class are readily ascertainable, as Defendant has access to Class Members' names and addresses affected by the Data Breach.

CAUSES OF ACTION
COUNT I: NEGLIGENCE
(On Behalf of Plaintiff and the Class)

194. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 193 above as if fully set forth herein.

195. Defendant required Plaintiff and Class Members to submit private, confidential Private Information to Defendant as a condition of receiving healthcare services from Defendant.

196. Plaintiff and Class Members provided certain Private Information to Defendant including their names, dates of birth, Social Security numbers, contact information medical and case histories, physicians' notes, drug use information, and other sensitive and confidential information about themselves.

197. Defendant had full knowledge of the sensitivity of the Private Information to which it was entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized persons. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that Private Information.

198. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices by Defendant.

199. Plaintiff and the Class Members had no ability to protect their Private Information

in Defendant's possession.

200. By collecting and storing Plaintiff's and Class Members' Private Information in its network server(s), Defendant had a duty of care to use reasonable means to secure and safeguard it, to prevent its unauthorized disclosure, and to safeguard it from theft. Defendant's duty included a responsibility to implement processes by which it could detect if that Private Information was exposed to the internet and to give prompt notice to those affected in the case of a data breach.

201. Defendant owed a duty of care to Plaintiff and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

202. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and its patients, which is recognized by statutes and regulations including but not limited to the FTC Act, HIPAA, and HITECH as well as the common law. Defendant was able to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach, yet failed to do so.

203. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

204. Pursuant to the FTC Act, 15 U.S.C. § 45 *et seq.*, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

205. Further, pursuant to HIPAA, 42 U.S.C. § 1302d *et seq*., Defendant had a duty to

implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

206. In additional, under HIPAA Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* 45 C.F.R. § 164.304.

207. Defendant breached its duties to Plaintiff and Class Members and violated the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

208. The injuries to Plaintiff and Class Members resulting from the Data Breach were directly caused by Defendant's violation of the statutes described herein.

209. Plaintiff and Class Members are within the class of persons the FTC Act and HIPAA were intended to protect.

210. The type of harm that resulted from the Data Breach was the type of harm the FTC Act and HIPAA were intended to guard against.

211. Defendant's failure to comply with the FTC Act and HIPAA and regulations constitutes negligence *per se*

212. Defendant's duty to use reasonable care in protecting Plaintiff's and Class Members' confidential Private Information in its possession arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to reasonably protect such Private Information.

213. Defendant's duty also arose from its position as a healthcare provider. Defendant holds itself out as a trusted provider of healthcare, and thereby assumes a duty to reasonably protect

its patients' information. Indeed, Defendant, as a healthcare provider, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members because of the Data Breach.

214. Defendant breached its duties, and was grossly negligent, by acts of omission or commission, by failing to use reasonable measures and indeed even minimally reasonable measures, to protect the Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately train employees on proper cybersecurity protocols;

c. Failing to adequately monitor the security of its networks and systems;

d. Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiff's and Class Members' Private Information;

f. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

215. But for Defendant's acts and omissions described above, constituting a wrongful and negligent breach of Defendant's duties owed to Plaintiff and Class Members, the Data Breach and Plaintiff's and Class Members' resulting injuries would have been avoided or at least, mitigated, including because Defendant would have identified the malicious activity and stopped the attack before the malicious actors had a chance to inventory Defendant's servers and exfiltrate files containing Plaintiff's and Class Members' Private Information.

216. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would cause Plaintiff's and Class Members'

injuries. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the industry.

217. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in one or more types of injuries to them.

218. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer a host of injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

219. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

220. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

221. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all Class Members.

COUNT II: BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

222. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 193 above as if fully set forth herein.

223. Defendant required Plaintiff and Class Members to provide and entrust their Private Information as a condition of obtaining healthcare services from Defendant.

224. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such Private Information and to timely and accurately notify Plaintiff and Class Members if and when their Private Information was breached and compromised.

225. Specifically, Plaintiff and Class Members entered into valid and enforceable implied contracts with Defendant when they agreed to provide their Private Information to Defendant.

226. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendant included Defendant's promise to protect Private Information it collected from Plaintiff and Class Members, or created on its own, from unauthorized disclosures. Plaintiff and Class Members provided this Private Information in reliance on Defendant's promise.

227. Under the implied contracts, Defendant promised and was obligated to (a) provide healthcare services to Plaintiff and Class Members; and (b) protect Plaintiff's and Class Members' Private Information that was provided to obtain such services and/or created in connection therewith. In exchange, Plaintiff and Class Members agreed to provide Defendant with payment and their Private Information.

228. Both the provision of payment and the protection of Plaintiff's and Class Members' Private Information were material aspects of these implied contracts with Defendant.

229. Defendant's contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information are also acknowledged, memorialized, and embodied in multiple documents, including Defendant's Notice of Privacy Practices, as described *supra*.

230. Defendant solicited and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

231. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act and HIPAA.

232. Plaintiff and Class Members who partnered or contracted with Defendant for healthcare services and who provided their Private Information to Defendant, reasonably believed and expected that Defendant would adequately employ adequate data security to protect that Private Information. Defendant failed to do so.

233. A meeting of the minds occurred when Plaintiff and the Class Members agreed to, and did, provide their Private Information to Defendant and agreed Defendant would receive payment for, amongst other things, the protection of their Private Information.

234. Plaintiff and Class Members performed their obligations under the contracts when they agreed to pay and provided their Private Information to Defendant.

235. Defendant materially breached its contractual obligations to protect the Private Information it required Plaintiff and Class Members to provide when it failed to implement even minimally reasonable logging and monitoring systems, data encryption protocols, or employee training, among other safeguards, and thus allowed Plaintiff's and Class Members' data to be disclosed to criminal actors bent on identity theft, fraud, and extortion.

236. Defendant materially breached its contractual obligations to deal fairly and in good faith with Plaintiff and Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify them of the Data Breach.

237. Defendant materially breached the terms of its implied contracts, including, but not limited to, by failing to comply with industry standards or the standards of conduct embodied in statutes like Section 5 of the FTC Act and HIPAA, or by failing to otherwise protect Plaintiff's and Class Members' Private Information, as set forth *supra*.

238. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct, by acts of omission or commission, in breach of these implied contracts with Plaintiff and Class Members.

239. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains with Defendant, and instead received services of a diminished value compared to that described in the implied contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

240. Had Defendant disclosed that its data security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have contracted with Defendant.

241. Plaintiff and Class Members would not have provided their Private Information to Defendant in the absence of the implied contracts between themselves and Defendant.

242. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

243. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely or adequate notice that their Private Information was compromised in and because of the Data Breach.

244. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class Members and the attendant Data Breach, Plaintiff and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Defendant.

245. Plaintiff and Class Members, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

246. Plaintiff and the Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide adequate credit monitoring to all Class Members.

COUNT III: BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

247. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 193 above as if fully set forth herein.

248. Given the relationship between Defendant, on one hand, and Plaintiff and Class Members, on the other hand, wherein Defendant served as a healthcare provider and guardian of Plaintiff's and Class Members' Private Information, Defendant was in a position of trust and confidence vis-à-vis Plaintiff's and Class Members and became their fiduciary in its undertaking to collect and maintain their Private Information.

249. As Plaintiff's and Class Members' fiduciary, Defendant was obligated to act

primarily for Plaintiff and Class Members to (a) safeguard their Private Information in its custody; (b) timely and adequately notify Plaintiff and Class Members of a Data Breach and disclosure of their Private Information; and (c) maintain complete and accurate records of what information (and where) Defendant did and does store.

250. Defendant had and has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their Private Information.

251. Due to the imbalance of power and superiority between themselves and Defendant, Plaintiff and Class Members placed their trust and confidence in Defendant, a sophisticated business entity and healthcare provider, to adequately safeguard the Private Information it collected and maintained from its patients.

252. Defendant accepted the trust and confidence placed in it by Plaintiff and Class Members and received their Private Information based on the mutual understanding that Defendant owed corresponding fiduciary duties to protect it from unauthorized disclosure.

253. Because of the highly sensitive nature of the Private Information they provided to Defendant, Plaintiff and Class Members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

254. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect their Private Information from unauthorized disclosure.

255. Defendant also breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach at all, let alone in a reasonable and practicable period.

256. As a direct and proximate result of Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, *inter alia*, following industry standard information security practices to secure Plaintiff's and Class Members' Private Information, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties in the Data Breach without Plaintiff's and Class Members' authorization.

257. The injuries and harm Plaintiff and Class Members suffered were the reasonably foreseeable result of Defendant's breach of its fiduciary duty to adequately secure Plaintiff's and Class Members' Private Information.

258. But for Defendant's wrongful disclosure of Plaintiff's and Class Members' Private Information in violation of the trust and confidence Plaintiff and Class Members placed in Defendant and Defendant's resulting fiduciary duties owed to Plaintiff and Class Members, their sensitive and confidential Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties in the Data Breach, and their injuries would have been avoided and/or mitigated.

259. As a direct and proximate result of Defendant's breaches of Plaintiff's and Class Members' confidence, Plaintiff and Class Members have suffered and will suffer injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

260. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

261. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) provide adequate credit monitoring to all Class Members.

COUNT IV: UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

262. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 193 above as if fully set forth herein.

263. This claim is pleaded in the alternative to the claim of breach of implied contract.

264. Plaintiff and Class Members conferred direct benefits upon Defendant in the form of agreeing to provide their Private Information to Defendant, without which Defendant could not perform the services it provides.

265. Defendant appreciated or knew of these benefits it received from Plaintiff and Class Members. Under principles of equity and good conscience, Defendant should not be allowed to retain the full value of these benefits—specifically, the costs it saved by failing to implement reasonable or adequate data security practices with respect to the Private Information it collected from Plaintiff and Class Members.

266. After all, Defendant failed to adequately protect Plaintiff's and Class Members' Private Information. And if such inadequacies were known, then Plaintiff and Class Members would never have agreed to provide their Private Information, or payment, to Defendant.

267. Defendant should be compelled to disgorge into a common fund, for the benefit of Plaintiff and the Class, all funds that were unlawfully or inequitably gained despite Defendant's

misconduct and the resulting Data Breach.

COUNT V: INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

268. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 193 above as if fully set forth herein.

269. Plaintiff and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to Defendant's protection of the Private Information in its possession from disclosure to unauthorized actors.

270. Defendant owed a duty to its patients, including Plaintiff and Class Members, to keep their Private Information confidential and secure.

271. Defendant failed to protect Plaintiff's and Class Members' Private Information and instead exposed it to unauthorized persons which is now publicly available, including through the publication of such information to the Dark Web where cybercriminals go to find their next identity theft and extortion victims.

272. Defendant allowed unauthorized third parties access to and examination of the Private Information of Plaintiff and Class Members, by way of Defendant's failure to protect the Private Information.

273. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and Class Members is highly offensive to a reasonable person and represents an intrusion upon Plaintiff's and Class Members' seclusion as well as a public disclosure of private facts.

274. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Private Information to Defendant as a condition of receiving healthcare services, but did so privately, with an intention that the Private

Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

275. Through the intrusion, Defendant permitted Plaintiff's and Class Members' Private Information to be published online to countless cybercriminals whose mission is to misuse such information, including through identity theft and extortion.

276. Defendant was fully aware that a failure to implement industry standard cybersecurity safeguards was substantially certain to lead to the disclosure of Plaintiff's and Class Members' sensitive Private Information.

277. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiff's and Class Members' interests in solitude or seclusion, as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

278. Thus, Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its information security practices were inadequate and insufficient.

279. Defendant acted with reckless disregard for Plaintiff's and Class Members' privacy when it allowed improper access to its systems containing Plaintiff's and Class Members' Private Information without protecting said data from the unauthorized disclosure, or even encrypting such information.

280. Defendant knew of the risk of a data breach but failed to adequately safeguard its systems to prevent the unauthorized release of Plaintiff's and Class Members' Private Information.

281. Because Defendant acted with this knowing state of mind, it had notice and knew of the inadequate and insufficient information security practices would injure and harm Plaintiff

and Class Members.

282. As a direct and proximate result of Defendant's acts and omissions set forth above, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer injuries and damages as set forth herein, including, without limitation, (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

283. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT VI: DECLARATORY RELIEF
(On Behalf of Plaintiff and the Class)

284. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 193 above as if fully set forth herein.

285. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are

tortious and violate the terms of the federal and state statutes described in this Complaint.

286. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard patients' PII and PHI and whether Defendant is currently maintaining data security measures that effectively protect Plaintiff and Class Members from further data breaches that compromise their Private Information.

287. Plaintiffs continue to suffer injuries due to their Private Information's compromise in Defendant's Data Breach and remain at imminent risk that further compromises of their Private Information will occur in the future given the publicity around the Data Breach and the nature and quantity of the Private Information stored by Defendant.

288. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure patients' Private Information and to timely notify victims of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

289. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ proper security protocols consistent with law and industry standards to protect patients' Private Information.

290. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendant's server. The risk of another such breach is real, immediate, and substantial. If another breach of Defendant's server occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the injuries such a further breach will cause are not readily quantified, and they

will be forced to bring multiple lawsuits to rectify the same conduct.

291. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs at Defendant, Plaintiffs will likely be subjected to substantial identity theft and other damages. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

292. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and the thousands of patients whose confidential information would be further compromised

PRAYER FOR RELIEF

WHEREFORE, Plaintiff April Butler, on individually and on behalf of all others similarly situated, prays for judgment as follows:

A. An Order certifying this case as a class action, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding injunctive relief in the form of additional technical and administrative

cybersecurity controls as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding attorneys' fees and costs, as allowed by law,

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

I. Any and all such relief to which Plaintiff and the Class are entitled.

JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury of all issues so triable.

Dated: August 5, 2024

Respectfully submitted,

By: */s/ Andrew A. Lemmon*

Andrew A. Lemmon (LA Bar No. 18302)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
5301 Canal Boulevard
New Orleans, LA 70124
Tel: (985) 783-6789
alemmon@milberg.com

Jeff Ostrow* (FL Bar No. 121452)
Kenneth J. Grunfeld* (PA ID No. 84121)
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
1 West Las Olas, Suite 500
Fort Lauderdale, Florida 33301
T: (954) 525-4100
F: (954) 525-4300
ostrow@kolawyers.com
grunfeld@kolawyers.com

* *Pro hac vice forthcoming*

Counsel for Plaintiff and the Proposed Class